Appln No. 09/690,066
Amdt date August 22, 2005
Reply to Office action of June 22, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A security system for secure printing of value-bearing items in a wide area computer network comprising:

a plurality of user terminals coupled to the computer network;

a database including information about one or more users using the plurality of terminals;

a plurality of cryptographic devices remote from the plurality of user terminals and coupled to the computer network, wherein the cryptographic devices include[[s]] a computer executable code for authenticating one or more users, wherein each of the plurality of cryptographic devices is programmable to service any of the plurality of user terminals; and

a plurality of security device transaction data stored in the database for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user, wherein the cryptographic device authenticates the identity of each user and authenticates the user for a role, the role limiting the user to a subset of operations performed by the system.

2. (Original) The system of claim 1, wherein the security device transaction data related to a user is loaded into the cryptographic device when the user requests to operate on a value bearing item.

3. (Canceled)

4. (Previously Presented) The system of claim 1, wherein the assumed role is a security officer role to initiate a key management function.

5. (Previously Presented) The system of claim 1, wherein the assumed role is a key custodian role to take possession of shares of keys.

6. (Previously Presented) The system of claim 1, wherein the assumed role is an administrator role to manage a user access control database.

7. (Previously Presented) The system of claim 1, wherein the assumed role is an auditor role to manage audit logs.

8. (Previously Presented) The system of claim 1, wherein the assumed role is a provider role to withdraw from a user account.

9. (Previously Presented) The system of claim 1, wherein the assumed role is a user role to operate on a VBI.

10. (Previously Presented) The system of claim 1, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

11. (Previously Presented) The system of claim 1, wherein the cryptographic device includes a state machine for determining a state corresponding to availability of one or more commands in conjunction with the role.

12. (Original) The system of claim 1, wherein the cryptographic device includes a data validation subsystem and an auto-recovery subsystem for allowing the device to verify that data is up to date and to automatically re-synchronize the device with the data.

13. (Original) The system of claim 1, wherein the cryptographic device is stateless.

14. (Original) The system of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized modification of data.

15. (Original) The system of claim 14, wherein the computer executable code prevents the unauthorized modification, substitution, insertion, and deletion of related data and cryptographically critical security parameters.

16. (Original) The system of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data.

17. (Original) The system of claim 16, wherein the data includes non-public contents of a postage meter, including plaintext cryptographic keys and other critical security parameters.

18. (Original) The system of claim 1, wherein the cryptographic device includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions.

19. (Original) The system of claim 1, wherein the cryptographic device includes a computer executable code for detecting errors and preventing a compromise of the transaction data or critical cryptographic security parameters as a result of the errors.

20. (Original) The system of claim 1, wherein at least one of the users is an enterprise account.

21. (Previously Presented) The system of claim 1, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

22. (Original) The system of claim 1, wherein the cryptographic device stores information about a number of last transactions in a respective internal register.

23. (Original) The system of claim 22, wherein the database stores a table including the respective information about a last transaction, a verification module to compare the information saved in the device with the information saved in the database.

24. (Original) The system of claim 1, wherein the database includes data for creating one or more indicium, account maintenance, and revenue protection.

25. (Original) The system of claim 24, wherein the data includes virtual meter information.

26. (Original) The system of claim 24, wherein the data includes ascending and descending registers data.

27. (Original) The system of claim 1, wherein the value bearing item is a mail piece.

28. (Original) The system of claim 27, wherein the mail piece includes a digital signature.

29. (Original) The system of claim 1, wherein the cryptographic device encrypts validation information according to a user request for printing a VBI.

30. (Original) The system of claim 27, wherein the cryptographic device generates data sufficient to print a postal indicium in compliance with postal service regulation on the mail piece.

31. (Original) The system of claim 1, wherein the value bearing item is a ticket.

32. (Original) The system of claim 1, wherein a bar code is printed on the value bearing item.

33. (Original) The system of claim 1, wherein the value bearing item is a coupon.

34. (Original) The system of claim 1, wherein the value bearing item is currency.

35. (Original) The system of claim 1, wherein the value bearing item is a voucher.

36. (Original) The system of claim 1, wherein the value bearing item is a traveler's check.

37. (Original) The system of claim 1, wherein each security device transaction data includes one or more of an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

38. (Original) The system of claim 1, wherein each security device transaction data includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign device status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

39. (Original) The system of claim 1 further comprising at least one more cryptographic device remote from the plurality of user terminals coupled to the computer network, wherein the at least one more cryptographic device includes a computer executable code for authenticating any of the plurality of users.

40. (Original) The system of claim 39, wherein the cryptographic device shares a secret with the at least one more cryptographic device.

41. (Original) The system of claim 39, wherein one of the plurality of cryptographic devices is a master device and generates a master key set (MKS).

42. (Original) The system of claim 41, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

43. (Original) The system of claim 42, wherein the MKS further includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

44. (Original) The system of claim 41, wherein the MKS is exported to other cryptographic devices by any cryptographic device.

45. (Original) The system of claim 1, wherein the database includes a user profile for a subset of the plurality of users.

46. (Original) The system of claim 45, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period.

47. (Original) The system of claim 11, wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative

state, an exporting shares state, an importing shares state, and an error state.

48. (Original) The system of claim 47, wherein the command corresponding to the operational state comprises commands for one or more of access control, session management, key management, and audit support.

49. (Original) The system of claim 1, wherein the cryptographic device is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

50. (Currently Amended) A method for secure printing of value-bearing items over a computer network having a plurality of user terminals, the method comprising ~~the steps of~~:

storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of user terminals;

securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals, wherein each of the cryptographic devices accesses data elements for any of the user terminals;

storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of the plurality of users; and

verifying that the requesting user is authorized to assume a role and to perform a corresponding operation, the role limiting the user to a subset of commands provided.

51. (Original) The method of claim 50 further comprising the step of loading a security device transaction data related to a user into one of the one or more of cryptographic devices when the user requests to operate on a value bearing item.

52. (Original) The method of claim 50 further comprising the step of authenticating the identity of each user.

53. (Canceled)

54. (Previously Presented) The method of claim 50, wherein the assumed role is a security officer role and the corresponding command is initiating a key management function.

55. (Previously Presented) The method of claim 50, wherein the assumed role is an administrator role to manage a user access control.

56. (Previously Presented) The method of claim 50, wherein the assumed role is an auditor role to manage audit logs.

57. (Previously Presented) The method of claim 50, wherein the assumed role is a provider role to authorize increasing credit for a user account.

58. (Previously Presented) The method of claim 50, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

59. (Previously Presented) The method of claim 50, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

60. (Previously Presented) The method of claim 50, further comprising the step of determining a state corresponding to availability of one or more commands in conjunction with the roles.

61. (Original) The method of claim 60, wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state.

62. (Original) The method of claim 50, further comprising the steps of verifying that the database is up to date.

63. (Original) The method of claim 62, further comprising the steps of automatically re-synchronizing each of the cryptographic devices with the database.

64. (Original) The method of claim 50, further comprising the step of preventing unauthorized modification of data.

65. (Original) The method of claim 64, wherein the step of preventing comprises preventing unauthorized modification, substitution, insertion, and deletion of postage related data and cryptographically critical security parameters.

66. (Original) The method of claim 50,further comprising the step of preventing unauthorized disclosure of data.

67. (Original) The method of claim 50, further comprising the step of ensuring the proper operation of cryptographic security and VBI related meter functions.

68. (Original) The method of claim 50, further comprising the steps of detecting errors and preventing a compromise of the transaction data or critical cryptographic security parameters as a result of the errors.

69. (Previously Presented) The method of claim 50, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

70. (Original) The method of claim 50, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

71. (Original) The method of claim 50, further comprising the step of storing data for creating an indicium, account maintenance, and revenue protection.

72. (Original) The method of claim 50, further comprising the step of printing a mail piece.

73. (Original) The method of claim 72, wherein the mail piece includes a digital signature.

74. (Original) The method of claim 72, wherein the mail piece includes a postage amount.

75. (Original) The method of claim 72, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

76. (Original) The method of claim 50, further comprising the step of printing a ticket.

77. (Original) The method of claim 50, further comprising the step of printing a bar code.

78. (Original) The method of claim 50, further comprising the step of printing a coupon.

79. (Original) The method of claim 50, further comprising the step of printing currency.

80. (Original) The method of claim 50, further comprising the step of printing a voucher.

81. (Original) The method of claim 50, further comprising the step of printing a traveler's check.

82. (Original) The method of claim 50, wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

83. (Original) The method of claim 50, further comprising the step of using a private key to sign device status responses and the VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

84. (Original) The method of claim 50, further comprising the step of sharing a secret with any of the other devices.

85. (Original) The method of claim 50, further comprising the step of generating a master key set (MKS).

86. (Original) The method of claim 85, wherein the step of generating the MKS comprises the steps of generating a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

87. (Original) The method of claim 86, further comprising the step of generating a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

88. (Original) The method of claim 85,further comprising the step of exporting the MKS to other cryptographic devices by any cryptographic device.

89. (Original) The method of claim 50, further comprising the step of storing a user profile for a subset of the plurality of users.

90. (Original) The method of claim 80, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period

91. (Original) The method of claim 50, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.

92. (Currently amended) A system for secure processing of value-bearing items (VBIs) in a computer network comprising:

a plurality of user terminals coupled to the computer network;

a database coupled to the network and remote from the plurality of user terminals for storing information about one or more users using the plurality of terminals; and

a server system coupled to the network including a plurality of cryptographic devices for performing secure VBI functions utilizing the information stored in the database, each of the plurality of cryptographic devices processes data for any of the user terminals,

wherein the cryptographic device authenticates the identity of a user and restricts services to the user based on stored information in the database.

93. (Original) The system of claim 92, wherein at least one of the users is an enterprise account.

94. (Original) The system of claim 92, further comprising a plurality of security device transaction data stored in the database for ensuring authenticity and authority of each of the plurality of users, wherein each transaction data is related to one of the plurality of users and the security device transaction data related to a user is loaded into the cryptographic device when the user requests a VBI function.

95. (Canceled)

96. (Previously Presented) The system of claim 92, wherein the assumed role is an administrator role to manage a user access control database.

97. (Previously Presented) The system of claim 92, wherein the assumed role is a provider role to authorize increasing credit for a user account.

98. (Previously Presented) The system of claim 92, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

99. (Original) The system of claim 92, wherein the cryptographic device stores information about a number of last transactions in a respective internal register, the database

stores a table including the respective information about a last transaction, a verification module to compare the information saved in the device with the information saved in the table.

100. (Original) The system of claim 92, wherein the database includes data for creating indicium, account maintenance, and revenue protection.

101. (Original) The system of claim 92, wherein the value bearing item is a mail piece.

102. (Original) The system of claim 92, wherein the mail piece includes a digital signature.

103. (Original) The system of claim 92, wherein the mail piece includes a postage amount.

104. (Original) The system of claim 92, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

105. (Original) The system of claim 92, wherein the value bearing item is a ticket.

106. (Original) The system of claim 92, wherein the value bearing item includes a bar code.

107. (Original) The system of claim 92, wherein the value bearing item is a coupon.

108. (Original) The system of claim 92, wherein the value bearing item is currency.

109. (Original) The system of claim 92, wherein the value bearing item is a voucher.

110. (Original) The system of claim 92, wherein the value bearing item is a traveler's check.

111. (Original) The system of claim 92, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

112. (Original) The system of claim 92, wherein each security device transaction data includes a private key, a public key, and a public key certificate, wherein the private key is used to sign device status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

113. (Original) The system of claim 92, wherein the cryptographic device is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

114. (Original) The system of claim 92, wherein the cryptographic device protects data using a stored secret.

115. (Original) The system of claim 114, wherein the secret is a password.

116. (Original) The system of claim 114, wherein the secret is a public/private key pair.

117. (Currently Amended) A method for secure processing of value-bearing items (VBIs) in a computer network including a plurality of user terminals the method comprising ~~the steps of~~:

storing information about one or more users using the plurality of terminals in a database coupled to the network and remote from the plurality of user terminals; and

performing secure VBI functions utilizing the information stored in the database by a cryptographic device remote from the plurality of user terminals, each of the plurality of cryptographic devices is programmable to service any of the plurality of user terminals,

wherein the cryptographic device authenticates the identity of the user and provides a specialized set of operations to the user based on user information in the database.

118. (Original) The method of claim 117 further comprising the step of storing a plurality of security device transaction data in the database wherein, each transaction data is related to one of the plurality of users.

119. (Original) The method of claim 118 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a VBI.

120. (Canceled)

121. (Previously Presented) The method of claim 117, wherein the assumed role is an administrator role to manage a user access control.

122. (Previously Presented) The method of claim 117, wherein the assumed role is a provider role to authorize increasing credit for a user account.

123. (Previously Presented) The method of claim 117, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

124. (Original) The method of claim 117, further comprising the step of printing a postage value including a postal indicium.

125. (Original) The method of claim 124, wherein the postal indicium comprises a digital signature.

126. (Original) The method of claim 124, wherein the postal indicium comprises a postage amount.

127. (Original) The method of claim 124, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

128. (Original) The method of claim 117, further comprising the step of printing a ticket.

129. (Original) The method of claim 117, further comprising the step of printing a bar code.

130. (Original) The method of claim 117, further comprising the step of printing a coupon.

131. (Currently Amended) A method for secure processing of a value bearing item on a computer network having a plurality of users using a plurality of computer terminals for connecting to the network and a plurality of cryptographic devices remote from the users and coupled to the network, each cryptographic device

executing a plurality of security device transactions, the method comprising ~~the steps of~~:

requesting by a user authorization for a role, the role restricting the user to less than a full set of commands;

assigning a security device transaction data to the requesting user, wherein the security device transaction data may be executed on any of the plurality of cryptographic devices;

authenticating the identity of the user;

granting the requested role;

issuing a command that is available for the requested role; and

executing the issued command[[.]],

wherein each of the plurality of cryptographic devices processes data for any user.

132. (Original) The method of claim 131, wherein at least one of the users is an enterprise account.

133. (Original) The method of claim 131, wherein the requested role is a provider role to authorize increasing credit for a user account.

134. (Original) The method of claim 131, wherein the requested role is a user role to perform expected IBIP postal meter operations.

135. (Original) The method of claim 131, wherein the requested role is a certificate authority role to allow a public key certificate to be loaded and verified.

136. (Original) The method of claim 131, further comprising the step of preventing unauthorized and undetected modification of data, including the unauthorized modification, substitution, insertion, and deletion of postage related data and cryptographically critical security parameters.

137. (Original) The method of claim 131, further comprising the step of preventing unauthorized disclosure of non-public contents of a postage meter, including plaintext cryptographic keys and other critical security parameters.

138. (Original) The method of claim 131, further comprising the step of ensuring the proper operation of cryptographic security and VBI related meter functions.

139. (Original) The method of claim 131, further comprising the steps of detecting errors and preventing a compromise of the transaction data and critical cryptographic security parameters as a result of the errors.

140. (Original) The method of claim 131, further comprising the step of providing indications of an operational state of a VBI meter.

141. (Original) The method of claim 131, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

142. (Original) The method of claim 131, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each cryptographic device;

storing a table including the information about a last transaction in the database; and

comparing the information saved in the respective device with the respective information saved in the database.

143. (Original) The method of claim 142, further comprising the step of loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

144. (Original) The method of claim 131, further comprising the step of storing data for creating indicium, account maintenance, and revenue protection.

145. (Original) The method of claim 131, further comprising the step of printing a postage value including a postal indicium.

146. (Original) The method of claim 145, wherein the postal indicium comprises a digital signature.

147. (Original) The method of claim 145, wherein the postal indicium comprises a postage amount.

148. (Original) The method of claim 145, wherein the postal indicium comprises an ascending register of used postage and a descending register of available postage.

149. (Original) The method of claim 131, further comprising the step of printing a ticket.

150. (Original) The method of claim 131, further comprising the step of printing a bar code.

151. (Original) The method of claim 131, further comprising the step of printing an image.

152. (Original) The method of claim 131, further comprising the step of printing a coupon.

153. (Original) The method of claim 131, further comprising the step of printing currency.

154. (Original) The method of claim 131, further comprising the step of printing a voucher.

155. (Original) The method of claim 131, further comprising the step of printing a traveler=s check.

156. (Original) The method of claim 131, wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

157. (Original) The method of claim 131, further comprising the step of using a private key to sign device status responses and the VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

158. (Original) The method of claim 131, further comprising the step of sharing a secret with all the other devices.

159. (Original) The method of claim 158, wherein the secret is a password.

160. (Original) The method of claim 158, wherein the secret is a public/private key pair.

161. (Original) The method of claim 131, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.